ABSTRACT OF THE DISCLOSURE

A mobile or other device connects to a server via a publicly accessible network such as the Internet. After installation upon the device, a virtual private network (VPN) client connects to the server and downloads a VPN profile. In one embodiment the device creates public/private key pairs and requests enrollment of a digital certificate. In another embodiment a digital certificate and public/private key pairs are provided. The device also receives a digital certificate from the server and verifies the server certificate by requesting the user to supply a portion of a fingerprint for the certificate. The invention further includes an automatic content updating (ACU) client that downloads a user profile for the VPN, requests certificate enrollment, and updates the VPN client and other applications when new content is available. A security service manager (SSM) server includes, or is in communication with, a Web server, multiple databases, an enrollment gateway and an internal certification authority (CA). A VPN policy manager application creates and manages VPN profiles and/or policies and communicates with the SSM server. The SSM server, which may reside on an enterprise intranet, may further communicate with one or more external CAs.